International Journal of Electrical, Computing Engineering and Communication (IJECC)

Vol. 1, Issue. 2, April – 2015 *ISSN (Online): 2394-8310*

Application of image hiding in mp4-video using steganography technique

[1]S.Sangareswari, [2]Mrs.V.Aruna

[1]UG student, Department of IT, Sri Vidya College of Engineering and Technology, Virudhunagar, INDIA

[2]Assistant Professor, Department of IT, Sri Vidya College of Engineering and Technology, Virudhunagar, INDIA

Abstract - Currently, Internet and digital media are getting more and more popular. The requirement of secure transmission of data also increased. Information hiding is the process of secretly embedding information inside a data source without changing its perceptual quality. In cryptography, once the data is decrypted the information secrecy will not exits any more. The traditional LSB modification technique by randomly dispersing the bits of the message in the image and thus making it harder for unauthorized people to extract the original message, is vulnerable to loss of valuable hidden secrete information. Here, an information hiding and extraction procedure is proposed for high resolution mp4 videos. Although mp4 videos are large in size but it can be transmitted from source to target over network after processing the source mp4 video by using these Information hiding and Extraction procedure securely.

Keywords-Video;frame;security;DCT;

1. INTRODUCTION

The Internet is always vulnerable to interception by unauthorized people over the world**.** The importance of reducing a chance of the information being detected during the transmission is being an issue now days [1].

The improving technology and the ubiquity of the internet have allowed more and more people to transmit data via the internet. The contents of the transmission can be in the form of words, voices, images, or even computer animation, some contents transmitted can be confidential data such as highly valued product design or war plans, so to product these contents from interceptor's attention, the information hiding technology thus emerged.

An information hiding and extraction procedure for mp4 videos is to embedd the secret message bits in DCT higher order coefficients. The secret information taken here is an gray scale image pixel values. The pixel values are converted to binary values and embedded those values in higher order coefficient value of DCT of mp4 video frames [1].

Information hiding is divided into steganography and digital watermarking. Steganography is the art or practice of concealing a message, image, or file within another message, image, or file. Steganography and cryptology are similar in the way that they both are used to protect important information. [1].

Now-a-days the term "Information Hiding" relates to both watermarking and steganography. Watermarking is the technique use to hide information in a digital object (video, audio or image) so that information is robust to adjustments or alterations. By watermarking, the mark itself is invisible or unnoticeable for the human vision system. In addition, it should be impossible to remove a watermark without degrading the quality of the data of the digital object. On the other hand, the main goal of steganography is to hide secret information in the other cover media (video, audio or image) so that the other persons will not notice the presence of information.

In steganography carrier medium is defined as the object that carries the hidden information. Stego-object is the resultant production of steganography that is transmitted to the destination. Stego-key is defined as the key used to extract the hidden data from the stego- object. Data may be embedded in various possible carriers like audio file, document, file headers, digital image and video.

Information hiding requirements include the following:

a. Imperceptibility- The video with data and original data source should be perceptually identical.
b. Robustness- The embedded data should survive any processing operation the host signal goes through and preserve its fidelity.
c.Capacity-Maximize data embedding payload.
d. Security- Security is in the key. [2]

2. STEGANOGRAPHY

Steganography is the type of hiding data that means "covered writing" it is taken from Greek word stego means "covered" and graphy means "to write".[5] Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. Generally, messages will appear to be something else: images, articles, shopping lists, or some other cover text and, classically, the hidden message may be in invisible ink between the visible lines of a private letter. The goal of steganography is to avoid drawing suspicion to the transmission of a hidden message. If suspicion is raised, then this goal is defeated. [3]

The advantage of steganography, over cryptography, is that messages do not attract attention to themselves. Cryptography protects the contents of a message, steganography can be said to protect both messages and communicating parties.

3. IMPLEMENTATION

An Mp4 video file is nothing but a sequence of high resolution image called frames. Each frame consisting of three channel of RGB. After collecting the frame we perform DCT (8x8 block) on any channel (say Rchannel) of the frames and embed the secret information bits in selected higher order coefficients. Each frame is processed by 8x8 Inverse DCT block processing and combined to get mp4 video with hided message. [1]

Decoding is done in reverse process of encoding.First each frame is extracted from the created MP4 stego video.Then perform 8x8 DCT block processing on the channel where secret information was embedded earlier.Finally the secret bit information's are extracted by subtracting from original DCT block processed values.

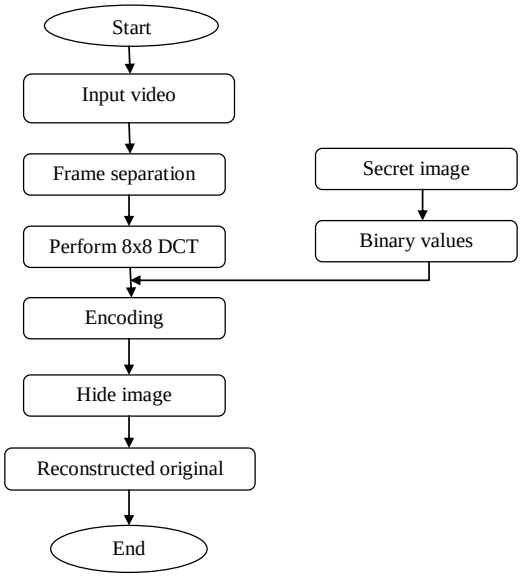


Figure 1 DATA FLOW DIAGRAM FOR ENCODING

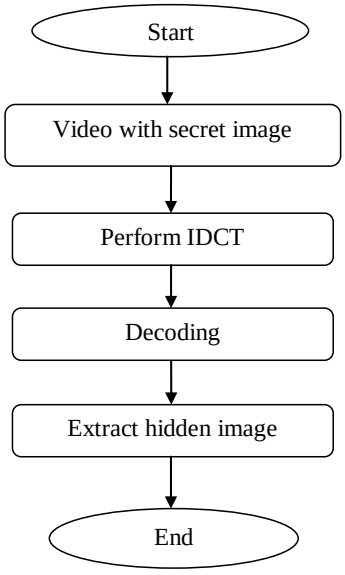


Figure 2 DATA FLOW DIAGRAM FOR DECODING

4. RSA ALGORITHM

The step by step process of the RSA algorithm is as follows:

1. Select two prime numbers x and y, multiple x and y and calculate the modulus, n=xy.
2. Select a third number e that is relatively prime to the product (x-1) (y-1).The number e is the public exponent.
3. Generate a private key by choosing a number d, which is multiple inverse of e mod ϕ (n).
4. Encrypt a message m, raise m to the power e under modulo n. The result is the cipher text(c).
5. Decrypt the cipher text, raise the cipher to the power d under modulo n.

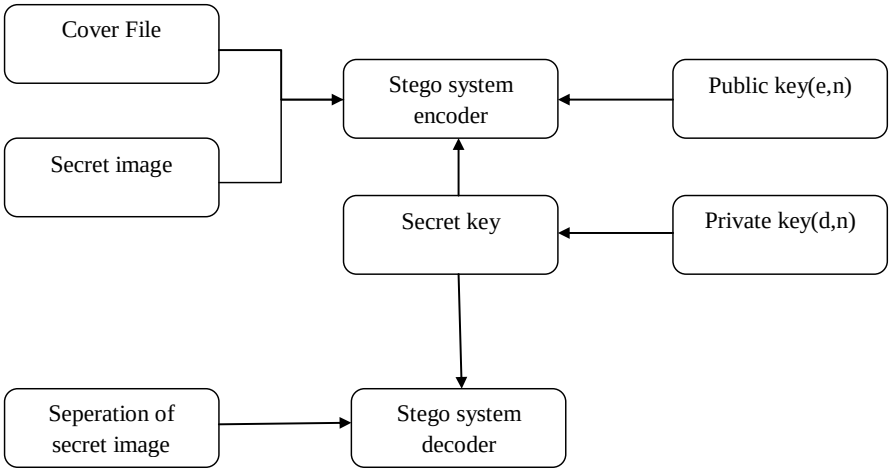


Figure 3 ARCHITECTURE DIAGRAM FOR RSA ALGORITHM

5. MODULE DISCRIPTION

5.1. Choosing secret image.
5.2.Frame extraction and hiding secret image.
5.3. Extract the original image from stego video.

5.1Choosing secret image:

An image is chosen and its pixel values are found to be 284x177. Each pixel intensity is then converted into equivalent binary values. If the size of the image is

284x177. Then the generated result is 284x177x8=402144 bit [1]

Figure 4 Secret image

The intensity pixel values are converted into binary value. Now converting 0's to -1 which gives binary values. Now multiply each bit with α (α=0.01). The JPEG method is used for both color and black & white images [4].

5.2. Frame extraction and hiding secret image:

In this scenario the mp4 video is considered as a cover or host video and all frames were extracted

(21 frames).324x244 is the resolution of original video. Then perform DCT on frames. But the original size of the image is 284x177 .So 300x168x8 bit should be encoded in this mp4 video frames per 8x8 DCT Higher order coefficients. The given input mp4 video pixel size is 324x244 is divided by 8x8 block size and after multiplied by 16 will get 19764 bits. The secret image size is 284x177x8 is divided by 19764 and hence nearly will be getting 21 frames. [4]

After encoding, the frames are combined to get the mp4 stego video file with embedded secret message. [1]

After encoding is completed stego file is created as a result. The created stego file is stored in the given specified destination place.The RSA algorithm is used for the key generation. In the key generation user have to give two prime numbers. Using that prime numbers the allowable private and public keys are displayed. The user can choose any one for d, e values. The n value will be generated for both the keys. The public key e and n values are used for the encryption.

5.3.Extract the original image from stego video:

First extract the mp4 video frames. R-channel frames are processed by 8x8 block IDCT.8x8 block processed R-Channel original frame values are subtracted to get secret message. From extracted secret message the image is reconstructed.

The stego file containing the hidden image is used as the cover file. The private key d and n values are used for the decryption. The hidden image is extracted from the stego file.

6.ANALYSING IMAGE QUALITY:

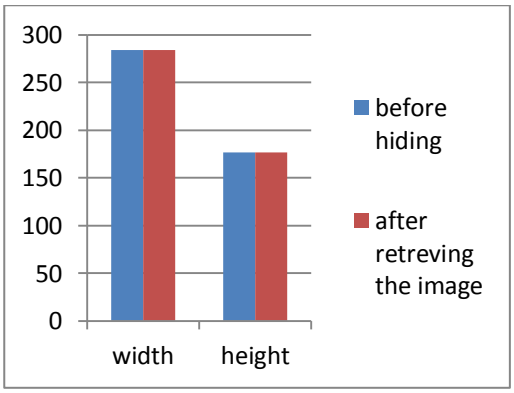
Before hiding the image the pixel value of original image is 284x177.

Figure 5 Image before hiding

After extract the original image from the stego video the quality does not changed. The pixel value is same as the original image(284x177).

Figure 6 Image after extracting from stego video

The quality representation of the image is shown in the graph. The quality of the image in terms of pixels of the original and retrieved image does not vary.



7. CONCLUSION

In this paper the information hiding technique has been applied in mp4 video to insert image secretly. More information can also be hidden in other channel of a frame giving more capacity of data to hide. Quality of the image after encoding is almost similar to the original.Future work may be the application of steganographic technique in various formats of video files with its robustness checked.

REFERENCE

1. Vandana Thakur, Monjul Saikia "Hiding Secret Image in Video" 2013 International Conference on Intelligent Systems and Signal Processing (ISSP)

2. Arup Kumar Bhaumik1, Minkyu Choi2, Rosslin J.Robles3, and Maricel O.Balitanas4 "Information hiding in Video" International
Journal of Database Theory and Application Vol.2,no.2,june

3. Nada Elya Tawfiq " Hiding Image within Video Clip" IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 11, Issue 6 (May. - Jun. 2013), PP 20-26

4. M. Suresh Kumar, G. Madhavi Latha "DCT Based Secret Image Hiding In Video Sequence" Int. Journal of Engineering Research and Applications ISSN : 2248-9622, Vol. 4, Issue 8(Version 1), August 2014, pp.05-09

5. E. Yuva Kumar, P. Padmaja "RSA Based Secured Image Steganography Using DWT Approach" *E.* Yuva Kumar Int. Journal of Engineering Research and Applications ISSN : 2248-9622, Vol. 4, Issue 8(Version 1), August 2014, pp.01-04